UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF TEXAS
AUSTIN DIVISION

UNITED STATES OF AMERICA, v. BAMEYI KELVIN OMALE, aka Leroy Brown, Henry Osas, Viktor Onye, Eddie Hassan, and Michael Abu, Defendant.	§ § § § § § § § § § § § §	No.: 1:19-CR-78-RP

GOVERNMENT'S SENTENCING MEMORANDUM

For the reasons set forth below as well as in other filings, the Government respectfully requests that the Court sentence Defendant BAMEYI KELVIN OMALE, aka Leroy Brown, Henry Osas, Viktor Onye, Eddie Hassan, and Michael Abu ("OMALE") to a sentence of 168 months or, if the court is not amenable to an above guideline range sentence, to a sentence at the top of the guideline range of 135 months.

Procedural Background

On April 2, 2019, the Defendant was charged with one count of Conspiracy to Commit Money Laundering. On September 24, 2019, the Defendant pleaded guilty without a plea agreement to the Conspiracy to Commit Money Laundering count, which carries a 0-20 year term of imprisonment.

Facts of the Offense

Beginning sometime before November 2016, OMALE, working with multiple other

individuals, began utilizing fraudulent foreign passports to open bank accounts in the Austin, Texas and Houston, Texas areas, as well as California. Those bank accounts were then used primarily to receive and launder the proceeds of Business Email Compromise ("BEC") scams—some proceeds of romance scams were also laundered through those bank accounts.

In BEC scams, the scammers target employees with access to company finances and trick them via email into making wire transfers to bank accounts thought to belong to trusted partners—except the money ends up in accounts controlled by money launderers associated with the fraudsters. Fraudsters use imitation email accounts to direct employees, customers, or partners of a victim company to send money to a bank account controlled by the fraudsters or a co-conspirator. Fraudsters often direct an employee, customer, or partner to wire funds under the disguise of legitimate business transactions, as in a payment to a new vendor.

In order to collect the fraudulent proceeds, BEC or romance fraudsters need bank accounts controlled by co-conspirators to collect the stolen money. The Defendant opened and controlled bank accounts that received the BEC funds. Defendant did so by acquiring fraudulent foreign passports in multiple names—including Leroy Brown, Henry Osas, Viktor Onye, Eddie Hassan, and Michael Abu —and then using those passports and other fake identification documents to open up P.O. Boxes in the Austin and Houston areas and also in California, often at a UPS Store. Once OMALE had a valid mailing address and fraudulent identification documents, Defendant would then open up bank accounts at various financial institutions in the Austin area. When the BEC scam was successful and a victim sent money to an account controlled by the conspiracy, Defendant or one of his co-conspirators acted quickly to remove any fraudulent funds deposited into the accounts they controlled.

The Defendant also connected other BEC scammers and money launderers with each

other, receiving a "cut" of the dirty money as payment. He also directed the actions of other members of the conspiracy and worked together to launder BEC fraud. For example, in June 2017 the Defendant used a fraudulent New Jersey driver's license to open up a Wells Fargo bank account in the name of Leroy Brown, Doing Business As: Shangdong Gumensa Metal Fabrication Co. with an Austin address. OMALE used the account to receive and quickly withdraw BEC funds. The account was closed by Wells Fargo in August 2017 after a $72,000 cashier's check was deposited into the Leroy Brown account ending in 8688. That cashier's check originated from a Wells Fargo bank account opened in the name of Stephen Wale by co-defendant and co-conspirator Nnamdi NWOSU in Austin, Texas.[1] NWOSU had utilized a fraudulent foreign passport in the name of Stephen Wale to open the account and a victim in Pennsylvania sent a wire transfer of $152,439.71 on or about July 31, 2017 to that bank account as a result of a BEC real estate scheme involving the victim's email being hacked. NWOSU then withdrew the fraudulently obtained funds via a $66,700 cashier's check and the aforementioned $72,000 cashier's check. Pictures from Wells Fargo show OMALE depositing the $72,000 cashier's check into his "Leroy Brown" Shangdong Gumensa Metal Fabrication Co. Wells Fargo account.

For the entire conspiracy, the total actual losses associated with the scheme was in excess of $5 million, with more than $10 million in attempted losses. More than $2 million dollars was deposited into accounts OMALE opened with fraudulent identification documents himself.

Response to Defendant's Objection to the PSR

Defendant objected to the PSR on the grounds that the 2-level increase for sophisticated

[1] NWOSU is still at-large as of the date of this sentencing memorandum.

means pursuant to U.S.S.G. §2B1.1(b)(10)(C) was duplicative of the 2-level increase for sophisticated laundering pursuant to U.S.S.G. §2S1.1(b)(2)(B). The Government opposes this objection because both increases are appropriate and not duplicative and because there are other grounds to apply U.S.S.G. §2B1.1(b)(10).

The underlying fraud offense is sophisticated due to the targeting of the companies, the hacking of the emails, the selection of the targets, and then the coordination for someone to receive the funds. The evidence shows that Defendant was involved in the fraud directly, as detailed below, and as relayed to the Government by cooperating witnesses. Accordingly, the 2-level increase for sophisticated means pursuant to U.S.S.G. §2B1.1(b)(10)(C) is correct and appropriate.

An analysis of the money laundering offense compared to the factors set out in the Sentencing Guidelines to determine if money laundering is "sophisticated" demonstrates that the actions of OMALE and the money laundering conspiracy were indeed "sophisticated" and worthy of the enhancement. Tracking the factors set out in the Guidelines, the money laundering is sophisticated due to the use of fake passports to open the bank accounts and the use of fake business names in "DBA" bank accounts (fictitious entities); the use of multiple hops of the money with fraud proceeds sent to one account, wired to another account in the U.S., and then sent abroad (two or more levels of transactions); and the use of foreign bank accounts in Nigeria (offshore financial accounts). Accordingly, the 2-level increase for sophisticated laundering pursuant to U.S.S.G. §2S1.1(b)(2)(B) is correct and appropriate.

For the above reasons, both sophisticated enhancements should apply. Because different conduct and different elements apply to each sophisticated enhancement, they are not duplicative.

U.S.S.G. §2B1.1(b)(10)(B) is an alternate means of increasing the offense level by 2, which would not insert the duplicative issues raised by Defense counsel. For U.S.S.G. §2B1.1(b)(10)(B) to apply, "a substantial part of a fraudulent scheme was committed from outside the United States." The facts in this case include a substantial number of the BEC hackers operating from outside of the United States.

The Government therefore requests that the Court deny Defendant's objection or apply U.S.S.G. §2B1.1(b)(10)(B) in the alternative—resulting in the same guideline range.

Defendant's Role

The conspiracy was a complex, sophisticated scheme that led to the loss of millions of dollars and attempted to steal millions more. OMALE was an active participant in and contributed significantly to the conspiracy's scheme by personally opening fraudulent bank accounts and receiving and withdrawing fraud funds, and by recruiting and hiring others to do the same. This Defendant was not an average participant—he actively recruited others to participate in this scheme and received an enormous sum of fraudulent proceeds.

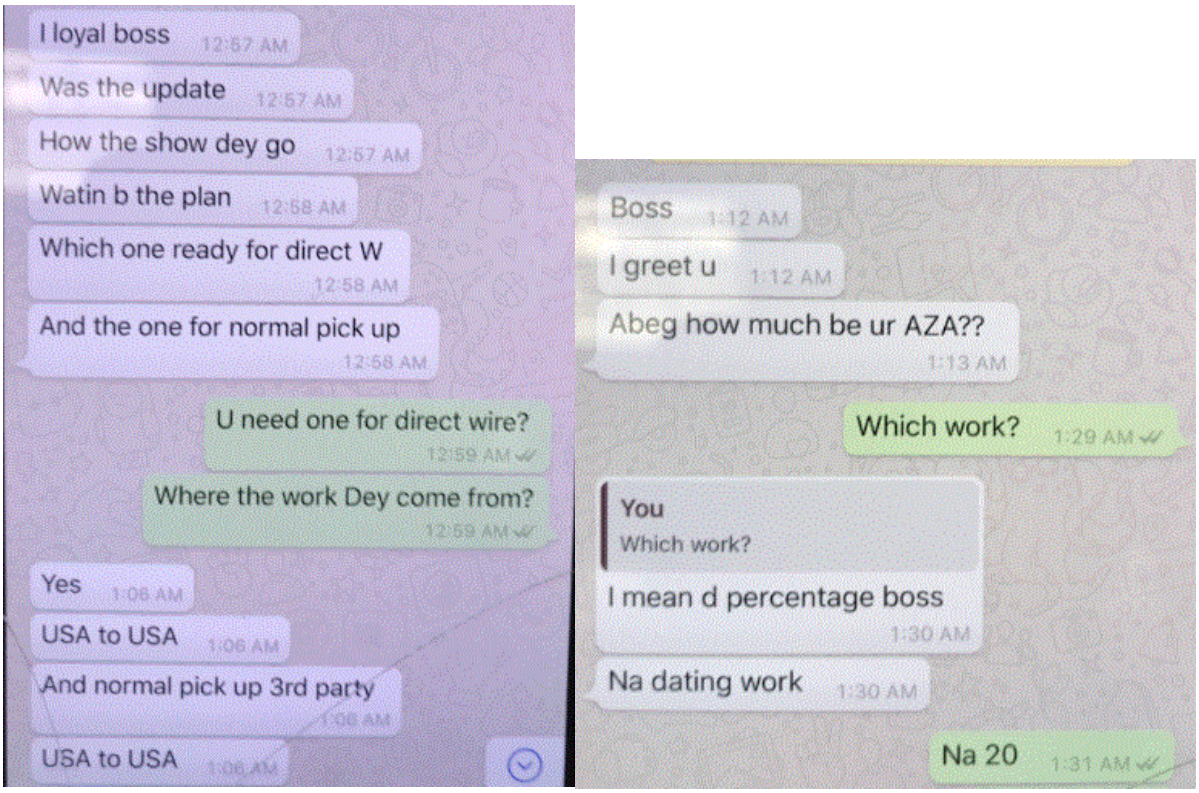
Examples of him not simply receiving money into accounts he opened with fraudulent documents occur throughout the investigation. On June 5, 2018, OMALE sent a message via WhatsApp to co-conspirator Joseph Odibobhahemen (hereinafter "Odibo") telling Odibo that "61k enter." Odibo then sent a message back showing that an account Odibo controlled received a wire transfer of $61,038.13. The very next day, after OMALE requests a phone call from Odibo, Odibo sent OMALE images showing that a bank account in the name of "John Ike" (which was later determined to have been opened by Odibo's co-defendant Onaghise who was working for Odibo) wired $49,800.35 from Round Rock, Texas to an entity in Nigeria.

Then on June 13, 2018, OMALE sent a screen shot from a computer displaying an email

exchange with a victim owner ("M.S.") of a company where M.S. said he just sent $26,217.63 for what M.S. believed were legitimate business expenses. In fact, M.S. had sent $26,217.63 to the "John Ike" account. The screen shot was sent from OMALE to Odibo, showing that OMALE was either directly committing the fraud or received the screen shot of the scam email from the scammer. Later on June 13, 2018, OMALE sent Odibo a message about a press release related to arrests made in Houston, Texas for BEC schemes.

These messages show that 1) OMALE is directly connected to the fraud (in contrast to claims made in his sentencing objection) and 2) OMALE was the one who hired Odibo to launder the proceeds for this particular fraud against M.S.

Importantly, OMALE did not just work with Odibo. The WhatsApp messages on OMALE's phone show a steady stream of money laundering, with OMALE requesting a 20 percent fee for his efforts. For example, the two chats below (OMALE's sent messages are in green/on the right-hand side) show OMALE open for money laundering business into bank accounts referred to as "aza" and open to doing "dating work" (romance scams) money laundering as well:



A series of messages between Odibo and OMALE from August 13, 2018 through August 22, 2018 show OMALE and Odibo working together to create a falsified invoice to a UK company for $105,545.65, pretending to be a Chinese company. The chat even includes a fake email exchange between the UK company and the Chinese company. A copy of the invoice is inserted below. The end of the chat is OMALE sharing a screen shot of his phone, logged into Wells Fargo, displaying a bank account under his control receiving a $105,545.65 deposit—that image is inserted below, too. The name of the company and relevant account numbers have been redacted to protect the victim.

Triumph [redacted] - UK Ltd
Meteor Business Park
[redacted] Road East
Gloucester
[redacted]
UK

Tel: +44 [redacted]

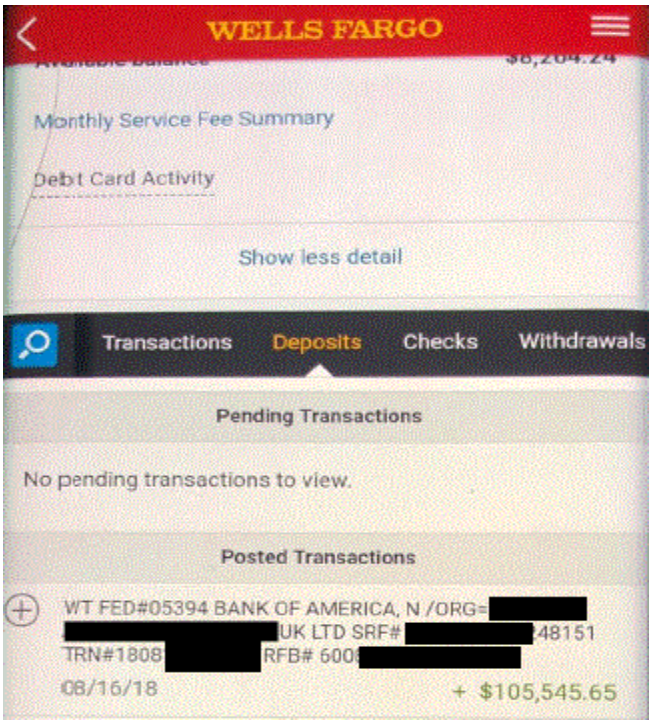
Reference Number	APP V002203
Wire Number	[redacted]
Page	1
Date	03/08/18

Supplier

[redacted]
Xin Tian Zhai WuDang District
GuiYang City
[redacted]
China 550018
CHINA

Date	Type	Our Reference	Your Reference	Amount
19/04/18	INVOICE	80042	10018049	12,560.60
13/04/18	INVOICE	80048	10018045	332.70
13/04/18	INVOICE	80049	10018044	25,472.69
13/04/18	INVOICE	80055	10018046	46,609.66
27/04/18	INVOICE	80060	100180528&2	20,570.00

Total to be paid by BACS **Total Amount:** 105,545.65



Request for Sentence

The scheme perpetrated by the Defendant and his co-conspirators—a BEC fraud—is rampant and growing throughout the United States. The U.S. Department of Treasury's Financial Crimes Enforcement Network recently reported that financial institution suspicious activity reporting demonstrated approximately $300 million in losses from BEC per month in 2018.[2] According to the FBI's Internet Crime Complaint Center (IC3), victims reported in excess of $26 billion in exposed dollar losses from BEC from June 2016 through July 2019.[3]

OMALE and his co-conspirators were a particularly effective network of BEC fraudsters and money launderers, perpetrating widespread financial harm to dozens of victims in the United States and around the world. A substantial sentence is necessary to serve as an appropriate deterrent. Especially to a Defendant like OMALE who took advantage of what the United States offered him—the chance to come to the United States legally—and used it to exploit others. The Defendant has pleaded guilty, but has offered no cooperation to the Government or provided any information to assist in the arrest or capture of co-conspirators still on the loose perpetrating these crimes to this day.

For the reasons outlined in this motion, the Government requests that Defendant be sentenced to at least 135 months imprisonment. There is a strong argument to be made that OMALE should be sentenced to an above-guideline sentence of 168 months based on his role in the offense and the need to deter other criminal conduct.

Conclusion

Defendant engaged in serious fraudulent and money laundering activity that deprived

[2] https://www.fincen.gov/news/news-releases/fincen-exchange-forum-counters-business-email-compromise-scams.
[3] https://www.ic3.gov/media/2019/190910.aspx

multiple victims of millions of dollars, and which attempted to deprive them of millions more. This type of activity is an increasing problem in our society. The Government therefore requests that Defendant be sentenced to 168 months imprisonment or, at least, a sentence at the top of the guideline range of 135 months.

Respectfully submitted,

JOHN F. BASH
United States Attorney

By:_____/s/_____
MICHAEL C. GALDO
KEITH M. HENNEKE
Assistant United States Attorneys

Certificate of Service

On February 10, 2020, I caused a true copy of the foregoing to be served on the Defendant's counsel of record *via* electronic mail and ECF.

/s/
MICHAEL C. GALDO
Assistant United States Attorney